



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709

7590

09/15/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

ALOMARI, FIRAS B

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 09/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,820	TARQUINI ET AL.	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on _____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

ET

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 06/27/2005 has been accepted.
2. The objection to the specifications is withdrawn as the application contained blanks with reference to related applications, but is remedied by filling them in.
3. Applicant's arguments filed 06/27/2005 have been fully considered but they are not persuasive.

Response to Arguments

1. The applicant's arguments regarding claims 1, 8 and 13 are not persuasive. As Vaidya discloses an operating system implemented either as software or as an actual hardware system operable to execute instructions (Col 6, lines 11-17) at the seven layers of the OSI model (Col 4, Lines 28-33 and Col 7, lines 20-25). Furthermore it is commonly known in the art that the OSI model includes seven layers (physical, Data Link, Network, Transport, Session, Presentation, Application). Additionally its known in the art that attack signatures in IDS is "a string of characters in the payload of a network message that indicate that the message contains malicious content, such as a virus, Trojan horse, or other intrusion activity" (See http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1321-00/en_US/HTML/install137.htm and http://www.webopedia.com/TERM/I/intrusion_signature.html) Which includes the present invention's text file defining network exploit rule.

2. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In this case, Vaidya discloses the attack signatures may have extra data like association data (Col 7, lines 54 through Col 8, line 14) or a timer/counter but he doesn't disclose a field for severity and enabled field on the other hand Walker discloses using the audit data as intrusion signatures (Col 4, lines 36-40) and he discloses the need to reduce the processing of those audit event (signatures) to the most important one (Col 4, lines 45-55) to reduce computational time when identifying an attack (Col 4, lines 55-61) to do so Walker discloses formatting the data record to comprise a type field and a primary discriminator (Col 11, lines 28-36) which includes the present invention enable filed to enable the system to identify which records need to be analyzed and what type of analysis needs to be performed (Col 11, lines 41-47) and a severity filed to identify which records are more critical to be analyzed than others (Col 12, lines 35-41), this ultimately leads to reduce the amount of data processed by the system and improve the performance of the signature matching step.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya US (6,279,113) in view of Walker US (6,134,664).

As per claim1: Vaidya discloses a node of a network for managing an intrusion protection system, the node comprising:
a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and (Col 6, Lines 3-11 and items 39,32 and 36 of FIG. 2)
an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application (Col 6, Lines 11-18 and Col 7, Lines 12-24), the management application operable to receive text-file input an input device (Col 7, lines 24-36, and Col 6, Lines 53-56), the text file defining a network exploit rule (Col 5, lines 33-38) but Vaidya doesn't explicitly disclose the file comprising at least one field. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion

Art Unit: 2136

detection engine (Col 4, Lines 37-40) where he formats the audit record to comprise plurality of fields (Col 11, Lines 29-35). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Vaidya system to use signatures files comprising at least one field. One would be motivated to do so in order to enable the system to identify different signatures and take different set of actions for the different signatures to improve the performance of the intrusion detection system.(Col 4, Lines 45-49)

As per claim 2: Vaidya doesn't explicitly disclose the node according to claim 1, wherein the network exploit rule further comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field. . However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he formats the audit record to comprise plurality of fields like a type of record field and a primary discriminator field (Col 11, Lines 29-35). Therefore it would be obvious to one ordinary skilled in the art at the time the invention was made to modify Vaidya system to use signatures files comprising at least one field. One would be motivated to do so in order to enable the system to identify different signatures and take different set of actions for the different signatures to improve the performance of the intrusion detection system.(Col 4, Lines 45-49)

As per claim 3: Vaidya discloses the node according to claim 1, wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the

Art Unit: 2136

machine-readable signature-file to at least one other node of the network. (Col 6, Lines 50-56)

As per claim 4, 9: The node according to claim 1, further comprising a database, the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database. (Col 6, Lines 3-7 and Col 5, Lines 47-65)

As per claim 5, 10: The node according to claim 2, further comprising a machine-readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files(Col 6, Lines 3-11), the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network. (Col 6, Lines 44-56)

As per claims 6, 11 and 17: Vaidya discloses the subset of the signatures include all the signatures of all nodes reside on that segment of the network but doesn't explicitly disclose the subset of signatures comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he formats the audit record to comprise plurality of fields (Col 11, Lines 29-35) and according to the value of a specific field in the record (Col 11, lines 42-

Art Unit: 2136

49) a decision whether to reduce the record or to forward the record for further consideration by the intrusion detection engine (Col 12, Lines 43-46) . Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to send signatures having an asserted enabled field value. One would be motivated to do so in order to enable the system to identify which signatures need to be used on that node which ultimately improve the performance of the intrusion detection system by reducing the number of signatures the node has to consider.(Col 4, Lines 45-49)

As per claims 7, 12 and 15: Vaidya doesn't explicitly disclose management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he eliminates records bases on a values or ranges of some fields in the record (Col 19, Lines 38-46) and a decision whether to reduce the record or to forward the record for further consideration by the intrusion detection engine is made based on those values (Col 12, Lines 43-46 and Col 20, lines 5-20). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to include a threshold value and process signatures having a severity value greater than the specified threshold to improve the performance. One would be motivated to do so in order to enable the

system to identify which signatures need to be used on that node and enable the system to weight records using barriers and boundaries (Col 4, Lines 29-33) which ultimately improve the performance of the intrusion detection system by reducing the number of signatures the node has to consider. (Col 4, Lines 45-49)

As per claim 8: Vaidya discloses a method of distributing command and security updates in a network having an intrusion protection system, comprising:
generating a text-file defining a network-exploit rule; (Col 5, Lines 33-39; Col 5, Lines 51-63 and Col 6, Lines 44-56)

but Vaidya doesn't explicitly disclose specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he formats the audit record to comprise plurality of fields like a type of record field and a primary discriminator field (Col 11, Lines 29-35). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Vaidya system to use signatures files comprising at least one field. One would be motivated to do so in order to enable the system to identify similar signatures and execute the same set of instructions for the similar signatures to improve the performance of the intrusion detection system by reducing the number of signatures the system have to examine.(Col 4, Lines 45-49)

Art Unit: 2136

As per claim 13: Vaidya discloses a computer-readable medium having stored thereon set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer; compiling the input into a machine-readable signature file (Col 5, lines 51-63) comprising machine-readable logic representative of the network-exploit rule (Col 5, Lines 33-39) and

but Vaidya doesn't explicitly disclose the signature file comprising a group of fields consisting of enabled field and severity field and evaluating the signature files based on those fields' values. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he include a value fields in the data records (Col 11, Lines 29-35) and eliminates records bases on a values or ranges of those fields in the record (Col 19, Lines 38-46) and a decision whether to reduce the record or to forward the record for further consideration by the intrusion detection engine is made based on those values (Col 12, Lines 43-46 and Col 20, lines 5-20). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to include a plurality of fields in the signature files and evaluating the signatures based on the values of those fields. One would be motivated to do so in order to enable the system to identify which signatures need to be used on that node which ultimately improve the performance of the intrusion detection system by reducing the number of signatures the node has to consider.(Col 4, Lines 45-49)

As per claim 14: Vaidya doesn't disclose the method of claim 13 comprising specifying a threshold value. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he eliminates records based on a specified values or ranges of some fields in the record (Col 19, Lines 38-46) and a decision whether to reduce the record or to forward the record for further consideration is made based on those values (Col 12, Lines 43-46 and Col 20, lines 5-20). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to enable the system to specify a threshold value and process signatures based on this value. One would be motivated to do so in order to enable the system to identify what signatures to use on a specific node which ultimately improve the performance of the intrusion detection system by reducing the number of signatures the node has to consider.(Col 4, Lines 45-49)

As per claim 16: Vaidya discloses the computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of generating a text-file from the input (Col 5, Lines 51-63 and Col 6, Lines 44-56), the text-file specifying the network-exploit rule (Col 5, lines 33-39)) but Vaidya doesn't explicitly disclose the file comprising at least one field. However Walker discloses a method for reducing native audit data or signatures for analysis by intrusion detection engine (Col 4, Lines 37-40) where he

Art Unit: 2136

formats the audit record to comprise plurality of fields (Col 11, Lines 29-35). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Vaidya system to use signatures files comprising at least one filed. One would be motivated to do so in order to enable the system to identify different signatures and take different set of actions for the different signatures to improve the performance of the intrusion detection system.(Col 4, Lines 45-49).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 8:30 am - 5:00 pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

Art Unit: 2136

FA


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100